UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

MARSHALL SMITH, BRANDON HERMAN, CHAD PATTERSON, JEFFERY ROBERTS, MICHAEL WILL, SUSAN WINSTEAD, ROBERT BOHANNON, HOLLY BUCKINGHAM, RICHARD MORELLO, JR., ROBERT HARRIS, AMANDA LARISCY, and CHARLES NEWMAN, individually and on behalf of all similarly situated persons, Plaintiffs, v. COMPLYRIGHT, INC., a Minnesota corporation, Defendant.	**Civil Action No. 1:18-cv-4990** **CLASS ACTION** **Jury Trial Demanded** **Hon. Edmond E. Chang**

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Plaintiffs Marshall Smith, Brandon Herman, Chad Patterson, Jeffery Roberts, Michael Will, Susan Winstead, Robert Bohannon, Holly Buckingham, Richard Morello, Jr., Robert Harris, Amanda Lariscy, and Charles Newman ("Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to themselves and on information and belief as to all other matters, by and through counsel, hereby bring this Consolidated Amended Class Action Complaint against defendant ComplyRight, Inc. ("ComplyRight" or "Defendant").

NATURE OF THE ACTION

1. Plaintiffs bring this class action against ComplyRight for its failure to implement and maintain reasonable security measures over personally identifiable information entrusted to

it—in particular, their name, address, telephone number, email address, and Social Security number (the "Personal Information").

2. On or around July 13, 2018, ComplyRight sent letters to Plaintiffs and many others around the country informing them that their Personal Information was accessed and viewed by unauthorized individuals while being maintained on ComplyRight's website (the "Data Breach"). The letter warned recipients: "your personal information that was accessed and/or viewed, [] may have been downloaded or otherwise acquired by an unauthorized user." The letter admits the Data Breach occurred from April 20, 2018 to May 22, 2018, but it may have gone on much longer, and it may have exposed more information than enumerated in the letter.

3. The letter also explained how ComplyRight came to be in possession of Plaintiffs' sensitive personal information: "Your personal information was entered onto our website by, or on behalf of, your employer or payer to prepare tax related forms, for example, Forms 1099 and W-2." Prior to receiving the letter, many recipients had never heard of ComplyRight or dealt with the company.

4. On information and belief, as a result of the Data Breach, Plaintiffs' and the other Class members' Personal Information, and perhaps more information, is now in the hands of unknown persons who intend to use it for criminal or nefarious purposes. On information and belief, the unauthorized persons have sold and will sell the Personal Information to exploit and injure Plaintiffs and the other Class members, to commit identity theft and identity fraud, and commit other acts injurious and detrimental to Plaintiffs and the other Class members. That was the reason that criminals sought out this lucrative information.

5. Criminals use information like the Personal Information to commit various crimes, such as opening fraudulent credit accounts, filing fraudulent income tax returns and diverting any

refund to the criminal's bank account, and impersonating the victim when arrested, obtaining medical services, and seeking employment. These crimes cause significant harm to the victims that can last for years, particularly where information as sensitive and valuable as Social Security numbers are involved.

6. The Data Breach was caused and enabled by ComplyRight's violation of its obligations to implement and maintain reasonable security measures to protect Personal Information from unauthorized access and disclosure and provide timely, adequate, and non-misleading notification of the Data Breach under the common law and statutory requirements imposed by state consumer protection and data breach notification laws.

PARTIES

7. Plaintiff Marshall Smith is a resident and citizen of California. On or about July 13, 2018, Mr. Smith received a letter from ComplyRight informing him that ComplyRight was subject to a "recent security incident involving some of [his] personal information that was maintained on [ComplyRight's] website." The letter further stated that his Personal Information "was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user," including his "name, address, telephone number, email address, and Social Security number." As a result of ComplyRight's failure to adequately safeguard Mr. Smith's Personal Information and timely notify him of the Data Breach, he has been injured and continues to suffer injuries.

8. Plaintiff Brandon Herman is a resident of West Hollywood, California. On or about July 13, 2018, Mr. Herman received a letter from ComplyRight informing him that ComplyRight was subject to a "recent security incident involving some of [his] personal information that was maintained on [ComplyRight's] website." The letter further stated that his Personal Information

"was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user," including his "name, address, telephone number, email address, and Social Security number." As a result of ComplyRight's failure to adequately safeguard Mr. Herman's Personal Information and timely notify him of the Data Breach, he has been injured and continues to suffer injuries.

9. Plaintiff Chad Patterson is a resident and citizen of California. On or about July 13, 2018, Mr. Patterson received a letter from ComplyRight informing him that ComplyRight was subject to a "recent security incident involving some of [his] personal information that was maintained on [ComplyRight's] website." The letter further stated that his Personal Information "was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user," including his "name, address, telephone number, email address, and Social Security number." As a result of ComplyRight's failure to adequately safeguard Mr. Patterson's Personal Information and timely notify him of the Data Breach, he has been injured and continues to suffer injuries.

10. Plaintiff Jeffery Roberts is a resident of New Port Richey, Florida. On or about July 17, 2018, Mr. Roberts received a letter informing him that ComplyRight was subject to a "recent security incident involving some of [his] personal information that was maintained on [ComplyRight's] website." The letter further stated that his Personal Information "was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user," including his "name, address, telephone number, email address, and Social Security number." As a result of ComplyRight's failure to adequately safeguard Mr. Roberts' Personal Information and timely notify him of the Data Breach, Mr. Roberts has been injured and continues to suffer injuries.

11. Plaintiff Michael Will is a resident of Marietta, Georgia. On approximately July 17, 2018, Mr. Will received a letter informing him that ComplyRight was subject to a "recent security incident involving some of [his] personal information that was maintained on [ComplyRight's] website." The letter further stated that his Personal Information "was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user," including his "name, address, telephone number, email address, and Social Security number." As a result of ComplyRight's failure to adequately safeguard Mr. Will's Personal Information and timely notify him of the Data Breach, he has been injured and continues to suffer injuries. Mr. Will has since purchased identity theft protection and monitoring from LifeLock.

12. Plaintiff Susan Winstead resides within the Northern District of Illinois and is a citizen of the State of Illinois. On July 17, 2018, Ms. Winstead received a letter informing her that ComplyRight was subject to a "recent security incident involving some of [her] personal information that was maintained on [ComplyRight's] website." The letter further stated that her Personal Information "was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user," including her "name, address, telephone number, email address, and Social Security number." As a result of ComplyRight's failure to adequately safeguard Ms. Winstead's Personal Information and timely notify her of the Data Breach, she has been injured and continues to suffer injuries.

13. Plaintiff Robert Bohannon resides in Granger, Indiana. On or about July 18, 2018, Mr. Bohannon received a letter informing him that ComplyRight was subject to a "recent security incident involving some of [his] personal information that was maintained on [ComplyRight's] website." The letter further stated that his Personal Information "was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized

user," including his "name, address, telephone number, email address, and Social Security number." As a result of ComplyRight's failure to adequately safeguard Mr. Bohannon's Personal Information and timely notify him of the Data Breach, he has been injured and continues to suffer injuries.

14. Plaintiff Holly Buckingham resides in Woodbine, Maryland. Sometime in July, Ms. Buckingham received a letter informing her that ComplyRight was subject to a "recent security incident involving some of [her] personal information that was maintained on [ComplyRight's] website." The letter further stated that her Personal Information "was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user," including her "name, address, telephone number, email address, and Social Security number." As a result of ComplyRight's failure to adequately safeguard Ms. Buckingham's Personal Information and timely notify her of the Data Breach, she has been injured and continues to suffer injuries.

15. Plaintiff Richard Morello, Jr. is a resident of Nevada. Plaintiff Morello is a self-employed web developer. Mr. Morello received a letter informing him that ComplyRight was subject to a "recent security incident involving some of [his] personal information that was maintained on [ComplyRight's] website." The letter further stated that his Personal Information "was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user," including his "name, address, telephone number, email address, and Social Security number." As a result of ComplyRight's failure to adequately safeguard Mr. Morello's Personal Information and timely notify him of the Data Breach, he has been injured and continues to suffer injuries. Mr. Morello called ComplyRight's telephone hotline to ascertain more information regarding the circumstances of his involvement with the Data Breach. He finally received a call back on July 30, 2018, which provided only scripted responses from an unhelpful

individual who was unable or unwilling to answer his questions. After that, Mr. Morello called a number of clients he felt comfortable asking and was informed that none of them used ComplyRight.

16. Plaintiff Robert Harris is a resident and citizen of New Mexico. On August 1, 2018, Mr. Harris received a letter informing him that ComplyRight was subject to a "recent security incident involving some of [his] personal information that was maintained on [ComplyRight's] website." The letter further stated that his Personal Information "was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user," including his "name, address, telephone number, email address, and Social Security number." As a result of ComplyRight's failure to adequately safeguard his Personal Information and timely notify him of the Data Breach, he has been injured and continues to suffer injuries.

17. Plaintiff Amanda Lariscy is a resident and citizen of Tennessee. On July 19, 2018, she received a letter informing her that ComplyRight was subject to a "recent security incident involving some of [her] personal information that was maintained on [ComplyRight's] website." The letter further stated that her Personal Information "was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user," including her "name, address, telephone number, email address, and Social Security number." As a result of ComplyRight's failure to adequately safeguard Ms. Lariscy's Personal Information and timely notify her of the Data Breach, she has been injured and continues to suffer injuries. Since the Data Breach, Ms. Lariscy has experienced instances of fraud. At least three fraudulent attempts to open accounts after the Data Breach were noticed. Also, fraudulent credit accounts were opened up in her name, using her Personal Information. Fraudulent transactions were noticed on existing accounts. An agent for one credit card company was able to advise Ms. Lariscy that one instance

of fraud was perpetrated in person without her credit card using her Personal Information. Ms. Lariscy filed numerous police reports, contacted numerous agents and customer service representatives, and took a day off of work to try and sort out the mess. She will continue to need to devote substantial time, effort, and resources to sort out the mess.

18. Plaintiff Charles Newman is a citizen of the State of Wisconsin who resides in Milwaukee County. Sometime in July 2018, Mr. Newman received a letter informing him that ComplyRight was subject to a "recent security incident involving some of [his] personal information that was maintained on [ComplyRight's] website." The letter further stated that his Personal Information "was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user," including his "name, address, telephone number, email address, and Social Security number." As a result of ComplyRight's failure to adequately safeguard Mr. Newman's Personal Information and timely notify him of the Data Breach, he has been injured and continues to suffer injuries.

19. Defendant ComplyRight, Inc. is a Minnesota corporation with its principal place of business in Pompano Beach, Florida.

JURISDICTION AND VENUE

20. The Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

21. Venue is proper in this District under 28 U.S.C. §§ 1391(b)(1) because defendant ComplyRight resides in this District.

FACTUAL BACKGROUND

22. ComplyRight offers a suite of legal compliance services for small businesses. Its website states: "At ComplyRight, our mission is to free employers from the burden of tracking and complying with the complex web of federal, state, and local employment laws, so they can stay focused on managing and growing their businesses." ComplyRight claims that it, among other things, "talk[s] to employers every day," "track[s] federal, state and local regulatory activity," and "consult[s] with [its] in-house legal research team to understand how employment regulations affect employers day-to-day." Its services range "[f]rom hiring and training to time tracking and recordkeeping, to labor law posting and tax information reporting."

23. Touting industry and regulatory certifications, and its adherence to same, ComplyRight advertises customer data security as a top priority.

24. Its website, located at https://www.complyright.com/products/tax-solutions (last visited September 10, 2018), displays the following:

25. ComplyRight's website boasts: "As a leading IRS-authorized provider of 1099, W-2, and ACA form processing services, we employ the latest, most sophisticated technologies and

best practices to ensure your sensitive data is protected end-to-end. These exacting measures and adherence to strict security standards ensure a superior level of data security and protection."

26. The site also states:

> ComplyRight Tax Solutions uses advanced 256-bit encryption technology to block the interception of sensitive data over the internet. Encryption alters the data before it is transmitted, making it unreadable until it is unlocked with a special cyber code after it is delivered to the authorized recipient. Data is password-protected and encrypted as soon as it's entered online and stays encrypted through the entire print, mail, and e-file process.
>
> - High-grade transport encryption protects electronic transmissions to the IRS and other government agencies
> - Includes encryption at rest to safeguard information stored in our systems
> - Effectively blocks interception of sensitive data

27. The website also represents:

> As a SOC-2-certified organization, we can promise:
>
> - Security – Our system is protected against unauthorized access, use, or modification
> - Availability – Our system is available for operation and use as committed or agreed upon
> - Processing integrity – Our data processing is complete, valid, accurate, timely and authorized
> - Confidentiality – confidential information is protected as committed or agreed upon
> - Privacy – Our processes for collecting, using, retaining, disclosing, and disposing of personal information conform with the commitments in our privacy notice, and with criteria established by the AICPA.

28. ComplyRight runs the website efile4biz.com. In order to convey the strength of its security, it says it is Geotrust and SOC certified, in HIPAA compliance, and authorized as an IRS e-file provider.

29. The website pays lip service to the need for adequate security to protect against the cyber threats facing its business, but only to lure potential clients:

> Due to the increasing threat of data breaches and identity theft in today's digitally focused world, you may question the security of e-filing. . . . As an industry leader and pioneer in online 1099, W-2, and ACA form processing, we employ the latest, most sophisticated security measures. The result is a level of data protection that would thwart even the most determined cyber criminals.
>
> . . .
>
> When it comes to risk-free e-filing, be aware that the IRS doesn't regulate how recipient data is handled. Instead, it's entirely up to the service provider. In turn, it's up to you to ask the right questions to be certain you're entrusting your 1099, W-2 and ACA recipient data to a security-conscious provider.

30. ComplyRight also touts its purported compliance with HIPAA:

> To ensure our policies and procedures meet HIPAA standards, we underwent an initial audit participate in annual audits, and provide ongoing support services for both employees and clients.
>
> As a HIPAA-compliant organization, we:
>
> - Ensure confidentiality, integrity and availability of all electronic PHI created, received, maintained, or transmitted
> - Includes encryption at rest to safeguard information stored in our systems
> - Protect against any reasonably anticipated uses or disclosures of PHI that are not permitted or required under the HIPAA Privacy Rule.

31. Despite these assurances and representations, ComplyRight failed to implement and maintain reasonable data security practices in accordance with its representations and the obligations it owes under the law.

32. On or around July 13, 2018, ComplyRight sent a letter out to Plaintiffs and numerous other persons stating in part:

> We are writing with important information about a recent security incident involving some of your personal information that was maintained on our website. Your personal information was entered onto our website by, or on behalf of, your employer or payer to prepare tax related forms, for example, Forms 1099 and W-2. We wanted to provide you with information regarding the incident, share the steps we have undertaken since discovering the incident, and provide guidance on what you can do to protect yourself.
>
> *What Happened?*

> On or about May 22, 2018, we initially learned of a potential issue involving our website. Upon learning of the potential issue, we disabled the platform and remediated the issue on the website.
>
> *What We Are Doing*
>
> In addition, we commenced a prompt and thorough investigation using external cybersecurity professionals. The forensic investigation concluded that there was unauthorized access to our website, which occurred between April 20, 2018 and May 22, 2018. After the extensive forensic investigation, a sophisticated review of our website, and analysis of potentially impacted individuals, on June 14, 2018 we discovered that some of your personal information was accessed and/or viewed. Although the forensic investigation determined that your information was accessed and/or viewed on the website, it could not confirm if your information was downloaded or otherwise acquired by an unauthorized user. We are not aware of any report of identity fraud as a direct result of this incident. Nevertheless, out of an abundance of caution we wanted to make you aware of the incident.
>
> *What Information Was Involved?*
>
> Your personal information that was accessed and/or viewed, and may have been downloaded or otherwise acquired, by an unauthorized user included your name, address, telephone number, email address, and Social Security number.

33. On information and belief, Plaintiffs and the other Class members' Personal Information was accessed, viewed, downloaded, acquired, and stolen by unauthorized persons from ComplyRight's website. The letter leaves open the possibility that other information was also compromised.

34. The letter is insufficient to comply with ComplyRight's obligations to provide adequate and timely notification of the Data Breach under the law. ComplyRight awaited a sophisticated and extensive forensic investigation when timely notification of the Data Breach was of the essence. ComplyRight kept the incident secret from Plaintiffs and the other Class members for nearly 2 months. Data thieves had 3 months from the alleged beginning of the Data Breach until notification to perpetrate fraud using the Personal Information with no victim aware of the threat.

35. The letter did not identify the number of affected individuals. However, Plaintiffs reasonably believe that the number of impacted individuals includes over 600,000 individuals.

36. Impacted individuals from around the country took to social media to raise concerns and questions about ComplyRight's confusing and concerning letter. ComplyRight's failure to provide any details to trusted news media or on its own website concurrently with the issuance of the letter created confusion and distrust among letter recipients, who largely have no idea who or what ComplyRight is, and suspect that the letter is fraudulent because they could find no mention of the incident online or in the news.

37. By all appearances, ComplyRight refused to respond to concerned individuals or news media, except through a heavily backlogged call center.

38. It did not take long for misinformation to spread online. Theories abound about the actual nature of the breach, whether it is legitimate or not, whether it is associated with other entities, or whether their employers ever actually used ComplyRight or any third party services related to tax preparation at all. This misinformation that filled in the void of ComplyRight's silence allows for phishing and other scams to seize advantage of those already victimized by the Data Breach.

39. Late Wednesday, July 18, 2018, ComplyRight finally provided largely the same information in an inconspicuous and difficult to access webpage on its website.

40. As a direct and foreseeable result of ComplyRight's failures, Plaintiffs' and the other Class members' Personal Information was placed onto unsecure and vulnerable online locations maintained by ComplyRight. The Personal Information (and perhaps more) was accessed, viewed, obtained, downloaded, and is now in the hands of unknown individuals intent on using the information to harm Plaintiffs and the other Class members.

Data Breaches Lead to Identity Theft

41. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.[1]

42. The Federal Trade Commission ("FTC") cautions that identity theft wreaks havoc on consumers' finances, credit history and reputation and can take time, money, and patience to resolve. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[2]

43. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[3] As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen private information directly on various Internet websites, making the information publicly available.

44. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

---

[1] See *Victims of Identity Theft, 2014*, DOJ, at 1 (2015), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Sept. 10, 2018).

[2] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

[3] Companies, in fact, also recognize Personal Information as an extremely valuable commodity akin to a form of personal property. *See* John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PERSONAL INFORMATION") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009).

45. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

46. ComplyRight's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

The Monetary Value of Privacy Protections and Personal Information

47. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[4]

48. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[5]

[4] Federal Trade Commission Public Workshop, *The Information Marketplace: Merging and Exchanging Consumer Data*, available at https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf (last visited Sept. 10, 2018).

[5] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Sept. 10, 2018).

49. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[6]

50. Recognizing the high value that consumers place on their Personal Information, many companies now offer consumers an opportunity to sell this information. The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their personal information.[7] This business has created a new market for the sale and purchase of this valuable data.[8]

51. Consumers place a high value not only on their personal information, but also on the privacy of that data. Researchers have already begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349."[9]

---

[6] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited Sept. 10, 2018).

[7] Steve Lohr, *You Want My Personal Data? Reward Me for It*, The New York Times, http://www.nytimes.com/2010/07/18/business/18unboxed.html (last visited Sept. 10, 2018).

[8] *See Web's Hot New Commodity: Privacy*, http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html (last visited Sept. 10, 2018).

[9] *See* Department of Justice, *Victims of Identity Theft, 2014*, at 6 (2015), https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Sept. 10, 2018).

52. The value of Plaintiffs' and the other Class members' Personal Information on the black market is substantial. By way of the Data Breach, ComplyRight has deprived Plaintiffs and Class members of the substantial value of their Personal Information. Rather than have an unknown third party realize the value of her Personal Information, Plaintiffs would choose to realize that value themselves.

Damages Sustained by Plaintiffs and the Other Class Members

53. Plaintiffs and other members of the Class have suffered injury and damages, including, but not limited to: (i) an increased risk of identity theft and identity fraud; (ii) identity theft and identity fraud; (iii) improper disclosure of their Personal Information, which is now in the hands of criminals; (iv) the value of their time, effort, and money spent mitigating the increased risk of identity theft and identity fraud; (v) the value of their time, effort, and expenses associated with mitigation, remediation, and sorting out the risk of fraud and actual instances of fraud; and (vi) deprivation of the value of their Personal Information, for which there is a well-established national and international market.

54. Plaintiffs and the other Class members have suffered and will continue to suffer additional damages based on the opportunity cost and value of time that Plaintiffs and the other Class members have been forced to expend and must expend in the future to monitor their financial accounts and credit files as a result of the Data Breach.

55. Acknowledging the damage to Plaintiffs and Class members, ComplyRight is instructing consumers to "remain vigilant in reviewing . . . financial account statements and credit reports for fraudulent or irregular activity." Plaintiffs and the other Class members now face a greater risk of identity theft.

CLASS ALLEGATIONS

56. Plaintiffs bring Counts I–III, as set forth below, on behalf of themselves and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a class (the "Nationwide Class") defined as:

> All persons whose Personal Information was maintained on ComplyRight's website during the Data Breach that occurred from at least April 20, 2018 through May 22, 2018, including all persons who were sent the July 13, 2018 letter informing them of the Data Breach.

Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

57. Plaintiffs Smith, Herman, and Patterson bring Counts IV–VI set forth below on behalf of themselves and a statewide class for California (the "California Class") defined as:

> All persons residing in California whose Personal Information was maintained on ComplyRight's website during the Data Breach that occurred from at least April 20, 2018 through May 22, 2018, including all persons who were sent the July 13, 2018 letter informing them of the Data Breach.

Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

58. Plaintiff Jeffery Roberts brings Counts VII set forth below on behalf of himself and a statewide class for Florida (the "Florida Class") defined as:

> All persons residing in Florida whose Personal Information was maintained on ComplyRight's website during the Data Breach that occurred from at least April 20, 2018 through May 22, 2018, including all persons who were sent the July 13, 2018 letter informing them of the Data Breach.

Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

59. Plaintiff Will brings Counts VIII–IX set forth below on behalf of himself and a statewide class for Georgia (the "Georgia Class") defined as:

> All persons residing in Georgia whose Personal Information was maintained on ComplyRight's website during the Data Breach that occurred from at least April 20, 2018 through May 22, 2018, including all persons who were sent the July 13, 2018 letter informing them of the Data Breach.

Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

60. Plaintiff Winstead brings Counts X–XII set forth below on behalf of herself and a statewide class for Illinois (the "Illinois Class") defined as:

> All persons residing in Illinois whose Personal Information was maintained on ComplyRight's website during the Data Breach that occurred from at least April 20, 2018 through May 22, 2018, including all persons who were sent the July 13, 2018 letter informing them of the Data Breach.

Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

61. Plaintiff Robert Bohannon brings Count XIII set forth below on behalf of himself and a statewide class for Indiana (the "Indiana Class") defined as:

> All persons residing in Indiana whose Personal Information was maintained on ComplyRight's website during the Data Breach that occurred from at least April 20, 2018 through May 22, 2018, including all persons who were sent the July 13, 2018 letter informing them of the Data Breach.

Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

62. Plaintiff Holly Buckingham bring Counts XIV–XVI set forth below on behalf of herself and a statewide class for Maryland (the "Maryland Class") defined as:

> All persons residing in Maryland whose Personal Information was maintained on ComplyRight's website during the Data Breach that occurred from at least April 20, 2018 through May 22, 2018, including all persons who were sent the July 13, 2018 letter informing them of the Data Breach.

Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

63. Plaintiff Richard Morello, Jr. brings Counts XVII–XIX set forth below on behalf of himself and a statewide class for Nevada (the "Nevada Class") defined as:

> All persons residing in Nevada whose Personal Information was maintained on ComplyRight's website during the Data Breach that occurred from at least April 20, 2018 through May 22, 2018, including all persons who were sent the July 13, 2018 letter informing them of the Data Breach.

Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

64. Plaintiff Robert Harris brings Counts XX–XXI set forth below on behalf of himself and a statewide class for New Mexico (the "New Mexico Class") defined as:

> All persons residing in New Mexico whose Personal Information was maintained on ComplyRight's website during the Data Breach that occurred from at least April 20, 2018 through May 22, 2018, including all persons who were sent the July 13, 2018 letter informing them of the Data Breach.

Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

65. Plaintiff Amanda Lariscy brings Counts XXII–XXIV set forth below on behalf of herself and a statewide class for Tennessee (the "Tennessee Class") defined as:

> All persons residing in Tennessee whose Personal Information was maintained on ComplyRight's website during the Data Breach that occurred from at least April 20, 2018 through May 22, 2018, including all persons who were sent the July 13, 2018 letter informing them of the Data Breach.

Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

66. Plaintiff Charles Newman brings Counts XXV–XXVI set forth below on behalf of himself and a statewide class for Wisconsin (the "Wisconsin Class") defined as:

> All persons residing in Wisconsin whose Personal Information was maintained on ComplyRight's website during the Data Breach that occurred from at least April 20, 2018 through May 22, 2018, including all persons who were sent the July 13, 2018 letter informing them of the Data Breach.

Excluded from the foregoing class are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

67. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

68. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** Class members are so numerous that joinder of all Class members would be impracticable. On information and belief,

Class members number in the hundreds of thousands. The precise number of Class members and their addresses are presently unknown to Plaintiffs, but may be ascertained from ComplyRight's own records. Class members may be notified of the pendency of this action by mail, email, Internet postings, or publication.

69. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class members and predominate over questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether ComplyRight failed to use reasonable care and reasonable methods to secure and safeguard Plaintiffs' and the other Class members' Personal Information;

b. Whether ComplyRight properly implemented its purported security measures to protect Plaintiffs' and the other Class members' Personal Information from unauthorized capture, dissemination, and misuse;

c. Whether ComplyRight took reasonable measures to determine the extent of the Data Breach after it first learned of same;

d. Whether ComplyRight provided timely and adequate notification of the Data Breach after it first learned of same;

e. Whether ComplyRight willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and Class members' Personal Information;

f. Whether ComplyRight was negligent in failing to properly secure and protect Plaintiffs' and the other Class members' Personal Information;

g. Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

70. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and the other Class members. Similar or identical common law and statutory violations, business practices, and injuries are involved.

Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

71. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other Class members because, among other things, all Class members were comparably injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. There are no defenses available to Defendant that are unique to Plaintiffs.

72. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate Class representatives because their interests do not conflict with the interests of the other Class members they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The other Class members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

73. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against ComplyRight, so it would be impracticable for Class members to individually seek redress for ComplyRight's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the

benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CLAIMS

COUNT I
Negligence
(On Behalf of the Nationwide Class)

74. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

75. ComplyRight owed numerous duties to Plaintiffs and the other members of the Class. These duties include the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Personal Information in its possession;

b. to protect Personal Information in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices and the practices and certifications represented on its website which it voluntarily undertook duties to implement; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly and sufficiently notifying Plaintiffs and the other members of the Class of the Data Breach.

76. ComplyRight knew or should have known the risks of collecting and storing Personal Information and the importance of maintaining secure systems. ComplyRight knew of the many breaches that targeted other entities in the years preceding the Data Breach, as illustrated by its own representations alleged herein.

77. Given the nature of ComplyRight's business, the sensitivity and value of the information it maintains, and the resources at its disposal, ComplyRight should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

78. ComplyRight knew or should have known that its systems did not adequately safeguard Plaintiffs' and the other Class members' Personal Information.

79. ComplyRight breached the duties it owed to Plaintiffs and Class members in several ways, including:

a. by failing to implement adequate security systems, protocols, and practices sufficient to protect Personal Information and thereby creating a foreseeable, unreasonable risk of harm;

b. by failing to comply with the minimum industry data security standards and its own assurances of superior data security standards;

c. by negligently performing voluntary undertakings to secure and protect the Personal Information it solicited and maintained; and

d. by failing to timely and sufficiently discover and disclose to consumers that their Personal Information had been improperly acquired or accessed, and providing misleading and unfounded suggestions that their information (and by extension their identity) is not in the immediate peril it is in fact in.

80. But for ComplyRight's wrongful and negligent breach of the duties it owed to Plaintiffs and the other Class members, their Personal Information would not have been compromised.

81. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of ComplyRight's negligent conduct. Plaintiffs and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

82. Plaintiffs' and the other Class members' injuries were proximately caused by ComplyRight's violations of the common law duties enumerated above, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT II
Negligence Per Se
(On Behalf of the Nationwide Class)

83. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

84. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses of failing to use reasonable measures to protect data collected on consumers. The FTC publications and orders described above also form and inform the basis of ComplyRight's duty.

85. ComplyRight violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. ComplyRight's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored, and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to Plaintiffs and the other Class members.

86. ComplyRight's violation of Section 5 of the FTCA constitutes negligence per se.

87. Plaintiffs and the other Class members are within the class of persons that the FTCA was intended to protect.

88. The harm that occurred as a result of the Data Breach is the type of harm that the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable security measures and avoid unfair or deceptive practices, caused the same type of harm that has been suffered by Plaintiffs and Class Members as a result of the Data Breach.

89. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of ComplyRight's violations of the FTC Act and similar state statutes.

Plaintiffs and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT III
Negligent Misrepresentation
(On Behalf of the Nationwide Class)

90. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

91. ComplyRight negligently misrepresented that it maintained and would continue to maintain adequate data privacy and security practices and procedures to safeguard Plaintiffs' and the other Class members' Personal Information from release, disclosure, and publication, and that it was equipped to protect it from foreseeable criminal attempts at unauthorized access.

92. Prior to and during the time ComplyRight was making these representations, it knew or should have known that it systems, policies, and practices, as described above, were not adequately designed, implemented, maintained, monitored, and tested to ensure that they in accordance with the representations, in accordance with legal obligations, or in accordance with what is necessary and reasonable to protect Plaintiffs' and the other Class members' Personal Information from release, disclosure, and publication, and fraudulent use for criminal purposes.

93. Plaintiffs and other reasonable persons, including the other Class members, reasonably relied on the misrepresentations set forth above, and in reasonable reliance thereon, engaged, used, and purchased ComplyRight's services and entrusted Plaintiffs' and the other Class members' Personal Information with ComplyRight.

94. Plaintiffs' and the other Class members' Personal Information would not have been entrusted to ComplyRight had they known the representations described above were false.

95. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of ComplyRight's negligent conduct. Plaintiffs and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT IV
Violation of California Customer Records Act,
California Civil Code §§ 1798.80, *et seq.* ("CRA")
(On Behalf of the California Class)

96. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

97. ComplyRight is a "business" within the meaning of California Civil Code § 1798.80(a).

98. Plaintiffs Smith, Herman, and Patterson and each member of the California Class are "individuals" within the meaning of California Civil Code § 1798.80(c).

99. California Civil Code § 1798.81.5 provides that a business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

100. The Personal Information of Plaintiffs and the other Class members that was provided to ComplyRight constitute computerized data that includes Personal Information that is owned, licensed, or maintained by ComplyRight.

101. ComplyRight failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

102. ComplyRight's failure to have reasonable measures in place to secure the Personal Information was grossly negligent.

103. ComplyRight violated the Customer Records Act by failing to notify California residents in the most expedient time possible and without unreasonable delay. ComplyRight learned of the Data Breach as early as May 22, 2018, but reasonably should have discovered it much earlier. Upon learning of the Data Breach, it failed to disseminate the required notification to Plaintiffs and the other Class members until around July 13, 2018.

104. Furthermore, the notification was insufficient, misleading, and not compliant with the law. It misrepresented the risks caused by the Data Breach, it had the appearance of a scam, and failed to provide adequate responses to inquiries by concealing the Data Breach from all other media and public forums. To the extent that the Data Breach happened to efile4biz, or other website, the Data Breach failed to accurately and sufficiently identify the relevant data collector.

105. California law gives the protection of its citizens' privacy the highest priority. Article 1, Section 1 of the California Constitution states that "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing and protecting property, and pursing and obtaining safety, happiness and privacy."

106. California's common law and statutory scheme also recognizes and protects California residents' right of privacy. For example, California Civil Code § 1798.81.5(a) states: It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own or license personal information about Californians to provide reasonable security for that information.

California citizens' rights to privacy have been compromised and infringed by the acts and

omissions of ComplyRight, as described herein.

107. Under § 1798.84 of the California Civil Code, any customer injured by a violation of this title may institute a civil action to recover damages. Any business that violates, proposes to violate, or has violated this title may be enjoined.

108. As a result of ComplyRight's violation of the Customer Records Act and the Data Breach, Plaintiffs and the other California Class members were injured and incurred actual harm and damages. Plaintiffs and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT V
Violation of the Unfair Competition Act,
Business & Professions Code § 17200, *et seq.* ("UCL")
(On Behalf of the California Class)

109. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

110. Plaintiffs bring this claim under the Unfair Competition Act (UCL), California Business & Professions Code § 17200, *et seq.*, on behalf of themselves and the California Class.

111. California Business & Professions Code § 17200, *et seq.* provides that unfair practices include, but are not limited to, "any unlawful, unfair or fraudulent business act[s] or practice[s]."

112. By and through its conduct, as described herein, ComplyRight engaged in activities that constitute unlawful, unfair and fraudulent business practices prohibited by California Business & Professions Code § 17200, *et seq.*

113. ComplyRight has committed acts of unfair competition, including those described above, by engaging in a pattern of "unlawful" business practices within the meaning of California

Business & Professions Code § 17200, *et seq.* Specifically, ComplyRight's conduct violates California Civil Code § 1798.80, *et seq.*, including but not limited to California Civil Code § 1798.81.5, 15 U.S.C. § 45, as well as others.

114. ComplyRight knew or should have known that failure to implement and maintain reasonable security procedures and practices to protect Plaintiffs' and the other Class members' Personal Information was unlawful, unfair, and fraudulent.

115. ComplyRight willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measures to prevent, detect, and mitigate the Data Breach.

116. ComplyRight made misrepresentations on its website as alleged herein regarding the strength and adequacy of its security measures when in fact its systems were vulnerable to unauthorized access. Moreover, ComplyRight's security measures were unable to detect any suspicious or unauthorized activity for a period of at least one month, and perhaps longer.

117. ComplyRight benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Data Breach.

118. ComplyRight's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiffs and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

119. Plaintiffs and the other Class members had no reasonable alternatives or chance to avoid the harm. Plaintiffs and the other Class members largely had no idea that ComplyRight maintained their information at all, let alone had the negotiating power individually to demand adequate data security.

120. ComplyRight failed to provide timely, adequate, and reasonable notification to Plaintiffs and the other Class members. Although discovering the Data Breach as early as May 22, 2018, ComplyRight did not distribute notification letters until nearly two months later. For two months the unauthorized individuals were allowed by ComplyRight to perpetrate significant criminal activities without Plaintiffs and the other Class members having an opportunity to defend themselves in any way. Furthermore, when the notification finally was sent, it was inadequate and caused confusion and distrust among Plaintiffs and the other Class members who had no idea who or what ComplyRight was. Because there has been no effort publicize the Data Breach through media or on its website (and by appearances efforts to conceal it), ComplyRight has failed in its duties to provide reasonable and effective notification to Plaintiffs and the other Class members.

121. ComplyRight's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

122. Plaintiffs and the other Class members have suffered actual damages including, identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

123. Plaintiffs' and the other Class members' injuries were proximately caused by ComplyRight's violations of the UCL, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

124. Plaintiffs and the other Class members are also entitled to injunctive relief in the form of adequate and sufficient notification of the Data Breach.

COUNT VI
California Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA")
(On Behalf of the California Class)

125. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

126. ComplyRight engaged in following prohibited conduct in violation of the California Consumer Legal Remedies Act, Cal. Civ. Code § 1770, among others:

a. Misrepresenting the source, sponsorship, approval, or certification of goods or services;

b. Representing that goods or services have characteristics that they do not have;

c. Representing that goods or services are of a particular standard quality, or grade when they are not;

d. Advertising goods or services with intent not to sell them as advertised; and

e. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

125. ComplyRight's representations and omissions were material and likely to mislead a reasonable consumer about the quality of its data security and ability to protect Personal Information.

126. Pursuant to Civil Code § 1782(d), Plaintiffs, individually and on behalf of the other Class members, seek a Court order enjoining the above-described wrongful acts and practices of ComplyRight, ordering ComplyRight to maintain reasonable security procedures to safeguard the Personal Information it collects and maintains, and ordering ComplyRight to provide accurate and non-misleading notice to Plaintiffs and the other Class members.

127. Pursuant to § 1782 of the Act, Plaintiffs notified ComplyRight in writing by certified mail of the particular violations of § 1770 of the Act and demanded that Defendant rectify

the problems associated with the actions detailed above and give notice to all affected consumers. A copy of the letter is attached as Group Exhibit A. If ComplyRight fails to provide accurate and non-misleading notice or to adopt reasonable security measures over the Personal Information it collects and maintains within 30 days of the date of written notice, Plaintiffs will amend this complaint to add claims for damages, as appropriate.

128. Plaintiffs and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them. Plaintiff Smith asserts a claim for actual damages.

129. Pursuant to § 1780(d) of the Act, attached hereto as Exhibit B is the affidavit showing that the action has been commenced in the proper forum.

COUNT VII
Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, *et seq.* ("FDUTPA")
(On Behalf of the Florida Class)

130. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

131. Plaintiff Roberts and the other Class members are consumers as defined under Fla. Stat. § 501.203.

132. ComplyRight advertised, offered, and sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

133. ComplyRight engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of § 501.204(1), in failing to properly implement adequate, reasonable security measures to protect their Personal Information and in failing to provide adequate, reasonable, and timely notification of the Data Breach.

134. ComplyRight willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measures to prevent, detect, and mitigate the Data Breach.

135. ComplyRight made misrepresentations on its website as alleged herein regarding the strength and adequacy of its security measures when in fact its systems were vulnerable to unauthorized access. Moreover, ComplyRight's security measures were unable to detect any suspicious or unauthorized activity for a period of at least one month, and perhaps longer.

136. ComplyRight benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Data Breach.

137. ComplyRight's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

138. Plaintiff and the other Class members had no reasonable alternatives or chance to avoid the harm. Plaintiff and the other Class members largely had no idea that ComplyRight maintained their information at all, let alone had the negotiating power individually to demand adequate data security.

139. ComplyRight failed to provide timely, adequate, and reasonable notification to Plaintiff and the other Class members. Although discovering the Data Breach as early as May 22, 2018, ComplyRight did not distribute notification letters until nearly two months later. For two months the unauthorized individuals were allowed by ComplyRight to perpetrate significant criminal activities without Plaintiff and the other Class members having an opportunity to defend themselves in any way. Furthermore, when the notification finally was sent, it was inadequate and

caused confusion and distrust among Plaintiff and the other Class members who had no idea who or what ComplyRight was. Because there has been no effort publicize the Data Breach through media or on its website (and by appearances efforts to conceal it), ComplyRight has failed in its duties to provide reasonable and effective notification to Plaintiff and the other Class members.

140. ComplyRight's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

141. Plaintiff and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

142. Plaintiff's and the other Class members' injuries were proximately caused by ComplyRight's violations of FDUTPA, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

143. Plaintiff and the other Class members are also entitled to injunctive relief in the form of adequate and sufficient notification of the Data Breach.

COUNT VIII
Georgia Security Breach Notification Act, O.C.G.A. § 10-1-912, *et seq.*
(On Behalf of the Georgia Class)

144. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

145. ComplyRight violated § 10-1-912 by failing to notify Plaintiff Will and the other Class members of the Data Breach in the most expedient time possible and without unreasonable delay. ComplyRight learned of the Data Breach as early as May 22, 2018, but reasonably should have discovered it much earlier. Upon learning of the Data Breach, it failed to disseminate the required notification to Plaintiff and the other Class members until July 13, 2018.

146. Furthermore, the notification was insufficient, misleading, and not compliant with the law. It misrepresented the risks caused by the Data Breach, it had the appearance of a scam, and failed to provide adequate responses to inquiries by concealing the Data Breach from all other media and public forums. To the extent that the Data Breach happened to efile4biz, or other website, the Data Breach failed to accurately and sufficiently identify the relevant data collector.

147. As a result of ComplyRight's unlawful conduct, Plaintiff and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

148. Plaintiff's and the other Class members' injuries were proximately caused by ComplyRight's violations, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

149. Plaintiff and the other Class members are also entitled to injunctive relief in the form of adequate and sufficient notification of the Data Breach.

COUNT IX
Georgia Uniform Deceptive Trade Practices Act, O.C.G.A. §§ 10-1-370, *et seq.*
(On Behalf of the Georgia Class)

150. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

151. ComplyRight engaged in deceptive trade practices in the conduct of its business, in violation of O.C.G.A. § 10-1-372(a), including:

a. Representing that good or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

152. ComplyRight's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and the other Class members' Personal Information;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures;

c. Failing to comply with common law and statutory during pertaining to the security and privacy of Plaintiff and the other Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and the other Class members' Personal Information;

e. Omitting suppressing, and concealing material facts that it did not reasonably maintain and implement adequate security of Personal Information.

153. ComplyRight's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of ComplyRight's data security and ability to protect the confidentiality of consumers' Personal Information.

154. ComplyRight intended to mislead Plaintiff and the other Class members and others and induce them to rely on its misrepresentations and omissions.

155. ComplyRight made misrepresentations on its website as alleged herein regarding the strength and adequacy of its security measures when in fact its systems were vulnerable to

unauthorized access. Moreover, ComplyRight's security measures were unable to detect any suspicious or unauthorized activity for a period of at least one month, and perhaps longer.

156. ComplyRight benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Data Breach.

157. ComplyRight's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

158. Plaintiff and the other Class members had no reasonable alternatives or chance to avoid the harm. Plaintiff and the other Class members largely had no idea that ComplyRight maintained their information at all, let alone had the negotiating power individually to demand adequate data security.

159. ComplyRight failed to provide timely, adequate, and reasonable notification to Plaintiff and the other Class members. Although discovering the Data Breach as early as May 22, 2018, ComplyRight did not distribute notification letters until nearly two months later. For two months the unauthorized individuals were allowed by ComplyRight to perpetrate significant criminal activities without Plaintiff and the other Class members having an opportunity to defend themselves in any way. Furthermore, when the notification finally was sent, it was inadequate and caused confusion and distrust among Plaintiff and the other Class members who had no idea who or what ComplyRight was. Because there has been no effort publicize the Data Breach through media or on its website (and by appearances efforts to conceal it), ComplyRight has failed in its duties to provide reasonable and effective notification to Plaintiff and the other Class members.

160. ComplyRight's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

161. Plaintiff and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

162. Plaintiff's and the other Class members' injuries were proximately caused by ComplyRight's violations of law, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

163. Plaintiff and the other Class members are also entitled to injunctive relief in the form of adequate and sufficient notification of the Data Breach.

COUNT X
Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. 505/2 ("ICFA")
(On Behalf of the Illinois Class)

164. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

165. Plaintiff Winstead and the other members of the Class were subjected to ComplyRight's unfair or deceptive acts or practices, in violation of 815 Ill. Comp. Stat. 505/2, in failing to properly implement adequate, reasonable security measures to protect their Personal Information and in failing to provide adequate, reasonable, and timely notification of the Data Breach.

166. ComplyRight willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measures to prevent, detect, and mitigate the Data Breach.

167. ComplyRight made misrepresentations on its website as alleged herein regarding the strength and adequacy of its security measures when in fact its systems were vulnerable to unauthorized access. Moreover, ComplyRight's security measures were unable to detect any suspicious or unauthorized activity for a period of at least one month, and perhaps longer.

168. ComplyRight benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Data Breach.

169. ComplyRight's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

170. Plaintiff and the other Class members had no reasonable alternatives or chance to avoid the harm. Plaintiff and the other Class members largely had no idea that ComplyRight maintained their information at all, let alone had the negotiating power individually to demand adequate data security.

171. ComplyRight failed to provide timely, adequate, and reasonable notification to Plaintiff and the other Class members. Although discovering the Data Breach as early as May 22, 2018, ComplyRight did not distribute notification letters until nearly two months later. For two months the unauthorized individuals were allowed by ComplyRight to perpetrate significant criminal activities without Plaintiff and the other Class members having an opportunity to defend themselves in any way. Furthermore, when the notification finally was sent, it was inadequate and caused confusion and distrust among Plaintiff and the other Class members who had no idea who or what ComplyRight was. Because there has been no effort publicize the Data Breach through

media or on its website (and by all appearances efforts to conceal it), ComplyRight has failed in its duties to provide reasonable and effective notification to Plaintiff and the other Class members.

172. ComplyRight's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

173. Plaintiff and the other Class members have suffered actual damages including improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

174. Plaintiff's and the other Class members' injuries were proximately caused by ComplyRight's violations of the Illinois Consumer Fraud Act, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

175. Plaintiff and the other Class members are also entitled to injunctive relief in the form of adequate and sufficient notification of the Data Breach.

COUNT XI
Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. 505/2RR
(On Behalf of the Illinois Class)

176. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

177. ComplyRight violated 815 Ill. Comp. Stat. 505/2RR(a)(1) by publicly posting or publicly displaying in any manner Plaintiff and the other Class members' Social Security number.

178. ComplyRight violated 815 Ill. Comp. Stat. 505/2RR(a)(3) by requiring Social Security numbers to be transmitted over the Internet without a secure connection or requiring encryption.

179. As a result of ComplyRight's conduct, Plaintiff and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Personal

Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

180. Plaintiff's and the other Class members' injuries were proximately caused by ComplyRight's violations of the Illinois Consumer Fraud Act, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT XII
Illinois Personal Information Protection Act,
815 Ill. Comp. Stat. 530/1, *et seq.* ("PIPA")
(On Behalf of the Illinois Class)

181. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

182. ComplyRight violated 815 Ill. Comp. Stat. 530/10(a) by failing to notify Illinois residents at no charge of the Data Breach in the most expedient time possible and without unreasonable delay. ComplyRight learned of the Data Breach as early as May 22, 2018, but reasonably should have discovered it much earlier. Upon learning of the Data Breach, it failed to disseminate the required notification to Plaintiff and the other Class members until July 13, 2018.

183. Furthermore, the notification was insufficient, misleading, and not compliant with the law. It misrepresented the risks caused by the Data Breach, it had the appearance of a scam, and failed to provide adequate responses to inquiries by concealing the Data Breach from all other media and public forums. To the extent that the Data Breach happened to efile4biz, or other website, the Data Breach failed to accurately and sufficiently identify the relevant data collector.

184. ComplyRight violated 815 Ill. Comp. Stat. 530/45 by failing to implement and maintain reasonable security measures to protect the Personal Information from unauthorized access, acquisition, destruction, use, modification, or disclosure. ComplyRight's security measures were unreasonable and inadequate to prevent or mitigate the scope and duration of the Data Breach,

were inadequate to detect the suspicious activity for an unreasonably long period of time, and were unable to ascertain the disposition of vast amounts of sensitive data. These unreasonable security measures caused, facilitated, and exacerbated the Data Breach and the damages that Plaintiff and the other Class members have incurred, are incurring, and will incur as a result of the Data Breach.

185. ComplyRight's violations constitute unfair or deceptive acts for which Plaintiff Winstead and the other Class members have a right of action under 815 Ill. Comp. Stat. 505/10.

186. Plaintiff and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach and violation of PIPA, including the increased risk of identity theft that resulted and continues to face them.

187. Plaintiff's and the other Class members' injuries were proximately caused by ComplyRight's violations of the PIPA, which were conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

188. Plaintiff and the other Class members are also entitled to injunctive relief in the form of adequate and sufficient notification of the Data Breach.

COUNT XIII
Violations of the Indiana Deceptive Consumer Sales Act
Ind. Code §§ 24-5-0.5-1, *et seq.* ("IDCSA")
(On Behalf of the Indiana Class)

189. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

190. ComplyRight is a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

191. ComplyRight is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A).

192. Plaintiff Bohannon and other members of the Class were subjected to ComplyRight's unfair, deceptive, and abusive acts or practices in violation of the IDCSA, in failing to properly implement adequate, reasonable security measures to protect their Personal Information and in failing to provide adequate, reasonable, and timely notification of the Data Breach.

193. ComplyRight willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measures to prevent, detect, and mitigate the Data Breach.

194. ComplyRight's representations and omissions include both implicit and explicit representations. For example, ComplyRight made misrepresentations on its website regarding the strength and adequacy of its security measures when in fact its systems were vulnerable to unauthorized access.

195. ComplyRight benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Data Breach.

196. ComplyRight's conduct alleged herein offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers. ComplyRight specifically violated the IDCSA, by engaging in, *inter alia*, the following conduct:

a. Failing to maintain sufficient security to keep Plaintiff's and the other Class members' sensitive Personal Information from being accessed and stolen;

b. Misrepresenting and fraudulently advertising (or omitting) material facts by representing and advertising that it would (or omitting that it would not) maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's

and the other Class members' Personal Information from unauthorized disclosure, release, data breaches, and theft;

c. Misrepresenting (or omitting) material facts to Plaintiff and the other Class members by representing and advertising that it did and would (or omitting that it would not) comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiff's and the other Class members' sensitive Personal Information;

d. Omitting, suppressing, and concealing the material fact of the inadequacy of the data privacy and security protections for Plaintiff's and the other Class members' Personal Information;

e. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Plaintiff's and the other Class members' sensitive Personal Information in violation of duties imposed by and public policies reflected in applicable federal and state laws, which resulted in the Data Breach. These unfair acts and practices violated duties imposed by laws including the FTC Act (15 U.S.C. § 45) and Indiana's data breach statute (Ind. Code § 24-4.9-3.5); and

f. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the data breach to Plaintiff and the other Class members in a timely and accurate manner, contrary to the duties imposed by Ind. Code § 24-4.9-3.3.

197. ComplyRight's acts and practices were "unfair" because they caused and were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

198. The injury to consumers from ComplyRight's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant number of consumers, but also because it inflicted a significant amount of harm on each consumer.

199. Plaintiff and the other Class members had no reasonable alternatives or chance to avoid the harm. Plaintiff and the other the other Class members largely had no idea that ComplyRight maintained their information at all, let alone had the negotiating power individually to demand adequate data security. By withholding important information from consumers about the inadequacy of its data security, ComplyRight created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury.

200. ComplyRight's acts and practices were "abusive" for numerous reasons, including:

a. Because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and ComplyRight concerning the state of its security (indeed, most Class members did not even know ComplyRight was handling their Personal Information); and

b. Because ComplyRight took unreasonable advantage of consumers' reasonable reliance that it would acting in their interests to secure their data.

201. ComplyRight also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

a. Misrepresenting that the subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have;

b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and if the supplier knows or should reasonably know that it is not; and

c. Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

202. ComplyRight's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of its data security and ability to protect the confidentiality of consumers' Personal Information.

203. As a direct and proximate result of ComplyRight's deceptive trade practices, Plaintiff and the other Class members suffered injuries, including the loss of their legally protected interest in the confidentiality and privacy of their Personal Information and damages.

204. The above unfair and deceptive practices and acts by Defendant were done as part of a scheme, artifice, or device with intent to defraud or mislead and constitute incurable deceptive acts under the IDCSA.

205. ComplyRight's conduct and acts are incurable for the reasons set forth herein, including but not limited to because Plaintiff's and the Class members' sensitive Personal Information—including their Social Security numbers—have been indefinitely exposed to the risk that this information will be used for nefarious purposes by fraudsters. Nothing that ComplyRight can or may do will cure this harm.

206. Indeed, as a self-touted expert in compliance, ComplyRight knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff's and the Class members' Personal Information and that risk of a data breach and data theft was highly likely. Given this knowledge, an intent to defraud was clearly present on the part of ComplyRight or it can be inferred from the circumstances.

207. ComplyRight acted intentionally, knowingly, and maliciously to violate the IDCSA, and recklessly disregarded Plaintiff and the other Class members' rights. ComplyRight was on notice that its security and privacy protections were inadequate given the multitude of recent high-profile data breaches. ComplyRight's actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, or other human failing.

208. Plaintiff and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

209. Plaintiff and the other Class members seek relief under Ind. Code § 24-5-0.5-4, including, not limited to damages, restitution, penalties, injunctive relief, reasonable attorneys' fees and costs, and punitive damages.

COUNT XIV
Violations of the Maryland Personal Information Protection Act
Md. Code, Com. Law §§ 14-3501, *et seq.* ("MPIPA")
(On Behalf of the Maryland Class)

210. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

211. Under the MPIPA, "[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and

practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations." Md. Code, Com. Law § 14-3503(a).

212. ComplyRight is a business that owns or licenses computerized data that includes Personal Information as defined by Md. Code, Com. Law §§ 14-3501(b)(1) and (2).

213. Plaintiff Buckingham and the other Class members are "individuals" and "customers" as defined and covered by §§ 14-3502(a) and 14-3503.

214. Plaintiff's and the other Class members' Personal Information includes Personal Information as covered under § 14-3501(d).

215. ComplyRight did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of § 14-3503.

216. The data breach was a "breach of the security of a system" as defined by § 14-3504(1).

217. Under § 14-3504(b)(1), "[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach."

218. Under §§ 14-3504(b)(2) and 14-3504(c)(2), "[i]f, after the investigation is concluded, the business determines that misuse of the individual's Personal Information has occurred or is reasonably likely to occur as a result of a breach of the security system, the business shall notify the individual of the breach" and that notification "shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system."

219. Because ComplyRight discovered a security breach and had notice of a security breach, it had an obligation to disclose the breach in a timely and accurate fashion as mandated by §§ 14-3504(b)(2) and 14-3504(c)(2). It did not do this, waiting multiple months to disclose and inform consumers of the breach.

220. By failing to disclose the breach in a timely and accurate manner, ComplyRight violated §§ 14-3504(b)(2) and 14-3504(c)(2).

221. As a direct and proximate result of ComplyRight's violations of the MPIPA, Plaintiff and the other Class members suffered damages, as described herein. As a result of ComplyRight's unlawful conduct, Plaintiff and the other Class members have suffered actual damages including, identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

222. Pursuant to § 14-3508, ComplyRight's violations of de §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the MCPA, Md. Code, Com. Law §§ 13-101, *et seq*. and subject to the enforcement and penalty provisions contained within the MCPA.

223. Plaintiff and the other Class members seek relief under Md. Code, Com. Law § 13-408, including actual damages and attorney's fees.

COUNT XV
Violations of the Maryland Social Security Number Privacy Act
Md. Code, Com. Law §§ 14-3401, *et seq.* ("MSSNPA")
(On Behalf the Maryland Class)

224. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

225. ComplyRight is a "person" as covered by Md. Code, Com. Law § 14-3402.

226. Plaintiff and the other Class members are "individual[s]" covered by § 14-3402.

227. Md. Code, Com. Law § 14-3402 prohibits a person from requiring an individual to transmit his/her Social Security number over the Internet unless the connection is secure or the individual's Social Security number is encrypted, and from initiating the transmission of an individual's Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted.

228. As described above, ComplyRight transmitted Plaintiff's and the other Class members' Social Security numbers over the Internet on unsecure connections and/or without encrypting the Social Security Numbers in violation of § 14-3402.

229. As a direct and proximate result of ComplyRight's violations of § 14-3402, Plaintiff and the other Class members suffered damages. As a result of ComplyRight's unlawful conduct, Plaintiff and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

230. Plaintiff and the other Class members seek relief under Md. Code, Com. Law § 14-3402, including actual damages and attorneys' fees.

COUNT XVI
Violations of the Maryland Consumer Protection Act
Md. Code, Com. Law §§ 13-101, *et seq.* ("MCPA")
(On Behalf of the Maryland Class)

231. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

232. ComplyRight is a person as defined by Md. Code, Com. Law § 13-101(h).

233. ComplyRight's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by § 13-101(i) and § 13-303.

234. Plaintiff Buckingham and the other Class members are "consumers" as defined by § 13- 101(c).

235. ComplyRight advertises, offers, or sell "consumer goods" or "consumer services" as defined by § 13-101(d).

236. ComplyRight advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

237. ComplyRight engaged in unfair and deceptive trade practices, in violation of Md. Code, Com. Law § 13-301, including:

a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

b. Representing that consumer goods or services have a characteristic that they do not have;

c. Representing that consumer goods or services are of a particular standard, quality, or grade that they are not;

d. Failing to state a material fact where the failure deceives or tends to deceive;

e. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;

f. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale, lease, or rental.

238. ComplyRight engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services or with respect to the provision of human resources services, in violation of Md. Code, Com. Law § 13-303, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and the other Class members' Personal Information, which was a direct and proximate cause of the ComplyRight data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the ComplyRight data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the other Class members' Personal Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and the MPIPA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and the other Class members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the other Class members' Personal Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and the MPIPA;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and the other Class members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the other Class members' Personal Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and the MPIPA.

239. ComplyRight's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of ComplyRight's data security and ability to protect the confidentiality of consumers' Personal Information.

240. Had ComplyRight disclosed that its data systems were not secure and, thus, vulnerable to attack, Plaintiff and the other Class members would have been able to protect themselves against ComplyRight's vulnerable systems (i.e., by avoiding their services) and ComplyRight would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, ComplyRight held itself out as a company that has expertise in legal compliance, and ComplyRight was trusted with sensitive and valuable Personal Information regarding thousands of consumers, including Plaintiff and the Class. ComplyRight accepted the responsibility of being a bailee of sensitive data while keeping the inadequate state of its security controls secret from the public.

241. ComplyRight acted intentionally, knowingly, and maliciously to violate the MCPA, and recklessly disregarded Plaintiff and the other Class members' rights. Given the large number of recent high-profile data breaches, ComplyRight was on notice that its security and privacy protections were inadequate.

242. As a direct and proximate result of ComplyRight's unfair and deceptive acts and practices, Plaintiff and the other Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including

from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

243. Plaintiff and the other Class members seek all monetary and nonmonetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

COUNT XVII
Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. § 598.0915, *et seq.*
(On Behalf of the Nevada Class)

244. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

245. Plaintiff Morello and the other members of the Class were subjected to ComplyRight's unfair or deceptive acts or practices, in violation of Nev. Rev. Stat. § 598.0915, *et seq.*, in failing to properly implement adequate, reasonable security measures to protect their Personal Information and in failing to provide adequate, reasonable, and timely notification of the Data Breach. Among other things, ComplyRight violated the following provisions of the Nevada Deceptive Trade Practices Act:

a. Knowingly making a false representation as to the source, sponsorship, approval or certification of goods or services for sale or lease (Nev. Rev. Stat. § 598.0915(2));

b. Knowingly making a false representation as to affiliation, connection, association with or certification by another person (Nev. Rev. Stat. § 598.0915(3));

c. Knowingly making a false representation as to the sponsorship, approval, status, affiliation or connection of a person therewith (Nev. Rev. Stat. § 598.0915(4));

d. Representing that goods or services for sale or lease are of a particular standard, quality or grade, or that such goods are of a particular style or model, if he or she knows or should know that they are of another standard, quality, grade or model

(Nev. Rev. Stat. § 598.0915(7));

e. Advertising goods or services for sale or lease with intent not to sell or lease them as advertised (Nev. Rev. Stat. § 598.0915(9));

f. Knowingly making any false representation in a transaction (Nev. Rev. Stat. § 598.0915(15);

g. Knowingly failing to disclose a material fact in connection with the sale or lease of goods or services (Nev. Rev. Stat. § 598.0923(2));

h. Knowingly violating a state or federal statute or regulation relating to the sale or lease of goods or services (Nev. Rev. Stat. § 598.0923(3));

246. ComplyRight willfully ignored the clear and present risk of a security breach of its systems and failed to implement and maintain reasonable security measures to prevent, detect, and mitigate the Data Breach.

247. ComplyRight made misrepresentations on its website as alleged herein regarding the strength and adequacy of its security measures when in fact its systems were vulnerable to unauthorized access. ComplyRight failed to disclose material facts regarding the lack of adequate and reasonable security measures it employed to protect highly sensitive Personal Information which it collected and aggregated on its website. Moreover, ComplyRight's security measures were unable to detect any suspicious or unauthorized activity for a period of at least one month, and perhaps longer.

248. ComplyRight knowingly violated state and federal statutes relating to the sale or lease of goods or services, including Nev. Rev. Stat. §§ 603A.020, *et seq.*

249. ComplyRight benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Data Breach.

250. ComplyRight's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

251. Plaintiff and the other Class members had no reasonable alternatives or chance to avoid the harm. Plaintiff and the other Class members largely had no idea that ComplyRight maintained their information at all, let alone had the negotiating power individually to demand adequate data security.

252. ComplyRight failed to provide timely, adequate, and reasonable notification to Plaintiff and the other Class members. Although discovering the Data Breach as early as May 22, 2018, ComplyRight did not distribute notification letters until nearly two months later. For two months the unauthorized individuals were allowed by ComplyRight to perpetrate significant criminal activities without Plaintiff and the other Class members having an opportunity to defend themselves in any way. Furthermore, when the notification finally was sent, it was inadequate and caused confusion and distrust among Plaintiff and the other Class members who had no idea who or what ComplyRight was. Because there has been no effort to publicize the Data Breach through media or on its website (and by appearances efforts to conceal it), ComplyRight has failed in its duties to provide reasonable and effective notification to Plaintiff and the other Class members.

253. ComplyRight's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and caused substantial injury to consumers.

254. As a result of ComplyRight's unlawful conduct, Plaintiff and the other Class members are victims of consumer fraud and have sustained actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information,

lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

255. Plaintiff's and the other Class members' injuries were proximately caused by ComplyRight's violations of the Nevada Deceptive Trade Practices Act.

256. Plaintiff and the other Class members are also entitled to injunctive relief in the form of adequate and sufficient notification of the Data Breach.

COUNT XVIII
Nevada Statutes Concerning Security of Information Maintained by Data Collectors and Other Businesses, Nev. Rev. Stat. §§ 603A.010, *et seq.*
(On Behalf of the Nevada Class)

257. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

258. ComplyRight is a business entity that handles, collects, disseminates and otherwise deals with nonpublic information. It is a "data collector" as defined under Nev. Rev. Stat. § 603A.030.

259. Plaintiff Morello's and the other Class members' name in combination with their social security number constitutes "personal information" under Nev. Rev. Stat. § 603A.040.

260. ComplyRight failed to implement and maintain reasonable security measures to protect Plaintiff's and the other Class members' personal information from unauthorized access, acquisition, destruction, use, modification or disclosure. ComplyRight's security measures were unreasonable and inadequate to prevent or mitigate the scope and duration of the Data Breach, were inadequate to detect the suspicious activity for an unreasonably long period of time, and were unable to ascertain the disposition of vast amounts of sensitive data. These unreasonable security measures caused, facilitated, and exacerbated the Data Breach and the damages that Plaintiff and the other Class members have incurred, are incurring, and will incur as a result of the Data Breach.

261. ComplyRight unlawfully transferred personal information through an electronic

nonvoice transmission other than a facsimile to a person outside of the secure system of the data collector without using encryption to ensure the security of electronic transmission.

262. ComplyRight unlawfully moved data storage devices containing personal information of Plaintiff and the other Class members beyond its logical or physical controls without using encryption to ensure the security of the information.

263. ComplyRight was grossly negligent in its conduct.

264. ComplyRight failed to provide timely, adequate, and reasonable notification to Plaintiff and the other Class members. Although discovering the Data Breach as early as May 22, 2018, ComplyRight did not distribute notification letters until nearly two months later. For two months the unauthorized individuals were allowed by ComplyRight to perpetrate significant criminal activities without Plaintiff and the other Class members having an opportunity to defend themselves in any way. Furthermore, when the notification finally was sent, it was inadequate and caused confusion and distrust among Plaintiff and the other Class members who had no idea who or what ComplyRight was. Because there has been no effort to publicize the Data Breach through media or on its website (and by appearances efforts to conceal it), ComplyRight has failed in its duties to provide reasonable and effective notification to Plaintiff and the other Class members.

265. Plaintiff and the other Class members have sustained actual damages, including identity theft improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT XIX
Unlawful Acts Regarding Social Security Numbers, Nev. Rev. Stat. § 205.4605
(On Behalf of the Nevada Class)

266. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

267. ComplyRight violated Nev. Rev. Stat. § 205.4605 by willfully and intentionally posting or displaying in any public manner Plaintiff's and the other Class members' Social Security number.

268. ComplyRight violated Nev. Rev. Stat. § 205.4605 by communicating or otherwise making available to the general public Plaintiff's and the other Class members' Social Security numbers and by requiring transmission of Plaintiff's and the other Class members' Social Security number over the Internet over an unsecure connection and unencrypted.

269. As a result of ComplyRight's conduct, Plaintiff and the other Class members have suffered actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

270. Plaintiff's and the other Class members' injuries were proximately caused by ComplyRight's violations of Nev. Rev. Stat. § 205.4605.

COUNT XX
New Mexico Unfair Practices Act, N.M. Stat. §§ 57-12-1, *et seq.* ("UPA")
(On Behalf of the New Mexico Class)

271. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

272. ComplyRight is a person engaged in trade and commerce as those terms are defined under the UPA, N.M. Stat. § 57-12-2.

273. The UPA prohibits unfair and deceptive acts and unconscionable acts in connection with the sale of goods or services in the regular course of its trade or commerce, including but not limited to:

a. Representing goods or services have sponsorship, approval, characteristics,

ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation or connection that the person does not have;

b. Representing that goods or services are of a particular standard, quality or grade or that goods are of a particular type or model if they are of another;

c. Using exaggeration, innuendo or ambiguity as to a material fact or failing to state a material fact if doing so deceives or tends to deceive;

d. Taking advantage of the lack of knowledge, ability, experience or capacity of a person to a grossly unfair degree;

e. Engaging in conduct that results in a gross disparity between the value received by Plaintiff and the other Class members and the price paid.

274. ComplyRight engaged in these unfair and deceptive trade practices by, among other things:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and the other Class members' Personal Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the other Class members' Personal Information,

including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and the MPIPA, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and the other Class members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the other Class members' Personal Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and New Mexico law;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and the other Class members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and the other Class members' Personal Information, including duties imposed by, *inter alia*, the FTC Act, 15 U.S.C. § 45, and New Mexico law.

275. ComplyRight's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of ComplyRight's data security and ability to protect the confidentiality of consumers' Personal Information.

276. Had ComplyRight disclosed that its data systems were not secure and, thus, vulnerable to attack, Plaintiff and the other Class members would have been able to protect themselves against ComplyRight's vulnerable systems (i.e., by avoiding their services) and ComplyRight would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, ComplyRight held itself

out as a company that has expertise in legal compliance, and ComplyRight was trusted with sensitive and valuable Personal Information regarding thousands of consumers, including Plaintiff and the Class. ComplyRight accepted the responsibility of being a bailee of sensitive data while keeping the inadequate state of its security controls secret from the public.

277. ComplyRight acted intentionally, knowingly, and maliciously to violate the UPA, and recklessly disregarded Plaintiff and the other Class members' rights. Given the large number of recent high-profile data breaches, ComplyRight was on notice that its security and privacy protections were inadequate.

278. As a direct and proximate result of ComplyRight's unfair and deceptive acts and practices, Plaintiff and the other Class members have suffered and will continue to suffer actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT XXI
New Mexico Privacy Protection Act, N.M. Stat. § 57-12B-1, *et seq.*
(On Behalf of the New Mexico Class)

279. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

280. ComplyRight violated N.M. Stat. § 57-12B-3, by acquiring or using social Security numbers of consumers and failing to adopt internal policies that limit access of Plaintiff's and the other Class members' Social Security numbers to those employees authorized to have access to that information to perform their duties; and failing to hold employees responsible if the Social Security numbers are released to unauthorized persons.

281. ComplyRight violated N.M. Stat. § 57-12B-4 by making the entirety of Plaintiff's

and the other Class members' Social Security number available to the general public.

282. As a result of ComplyRight's violation of the foregoing provisions, Plaintiff and the other Class members have suffered and will continue to suffer actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT XXII
Violation of the Tennessee Consumer Protection Act,
Tenn. Code. §§ 47-18-101, *et seq.* ("TCPA")
(On Behalf of the Tennessee Class)

283. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

284. ComplyRight engaged in unlawful, unfair, and deceptive acts or practices affecting the conduct of trade and commerce in violation of the Tennessee Consumer Protection Act. ComplyRight's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and the other Class members' Personal Information;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures;

c. Failing to comply with common law and statutory requirements pertaining to the security and privacy of Plaintiff and the other Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and the other Class members' Personal Information;

e. Omitting suppressing, and concealing material facts that it did not reasonably maintain and implement adequate security of Personal Information.

285. ComplyRight's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of ComplyRight's data security and ability to protect the confidentiality of consumers' Personal Information.

286. ComplyRight intended to mislead Plaintiff and the other Class members and others and induce them to rely on its misrepresentations and omissions.

287. ComplyRight made misrepresentations on its website as alleged herein regarding the strength and adequacy of its security measures when in fact its systems were vulnerable to unauthorized access. Moreover, ComplyRight's security measures were unable to detect any suspicious or unauthorized activity for a period of at least one month, and perhaps longer.

288. ComplyRight benefitted from not taking preventative measures and implementing adequate security measures that would have prevented, detected, and mitigated the Data Breach.

289. ComplyRight's failure to implement and maintain reasonable security measures caused and continues to cause substantial injury to Plaintiff and the other Class members that is not offset by countervailing benefits to consumers or competition or reasonably avoidable by consumers.

290. Plaintiff Lariscy and the other Class members had no reasonable alternatives or chance to avoid the harm. Plaintiff and the other Class members largely had no idea that ComplyRight maintained their information at all, let alone had the negotiating power individually to demand adequate data security.

291. ComplyRight failed to provide timely, adequate, and reasonable notification to Plaintiff and the other Class members. Although discovering the Data Breach as early as May 22, 2018, ComplyRight did not distribute notification letters until nearly two months later. For two months the unauthorized individuals were allowed by ComplyRight to perpetrate significant

criminal activities without Plaintiff and the other Class members having an opportunity to defend themselves in any way. Furthermore, when the notification finally was sent, it was inadequate and caused confusion and distrust among Plaintiff and the other Class members who had no idea who or what ComplyRight was. Because there has been no effort publicize the Data Breach through media or on its website (and by appearances efforts to conceal it), ComplyRight has failed in its duties to provide reasonable and effective notification to Plaintiff and the other Class members.

292. ComplyRight's conduct offends public policy and is immoral, unethical, oppressive, and unscrupulous, and causes substantial injury to consumers.

293. As a result of ComplyRight's unlawful conduct, Plaintiff and the other Class members have suffered and will continue to suffer actual damages, including improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

294. Plaintiff's and the other Class members' injuries were proximately caused by ComplyRight's violations of the law, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

295. Plaintiff and the other Class members are also entitled to injunctive relief in the form of adequate and sufficient notification of the Data Breach.

COUNT XXIII
Tennessee Personal Consumer Information Release Act,
Tenn. Code §§ 47-18-2107, *et seq*.
(On Behalf of the Tennessee Class)

296. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

297. ComplyRight violated Tenn. Code § 47-18-2107 by failing to notify Plaintiff and the other Class members of the Data Breach in the most expedient time possible and without

unreasonable delay. ComplyRight learned of the Data Breach as early as May 22, 2018, but reasonably should have discovered it much earlier. Upon learning of the Data Breach, it failed to disseminate the required notification to Plaintiff and the other Class members until July 13, 2018.

298. Furthermore, the notification was insufficient, misleading, and not compliant with the law. It misrepresented the risks caused by the Data Breach, it had the appearance of a scam, and failed to provide adequate responses to inquiries by concealing the Data Breach from all other media and public forums. To the extent that the Data Breach happened to efile4biz, or other website, the Data Breach failed to accurately and sufficiently identify the relevant data collector.

299. As a result of ComplyRight's unlawful conduct, Plaintiff and the other Class members have suffered and will continue to suffer actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

300. Plaintiff's and the other Class members' injuries were proximately caused by ComplyRight's violations, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

301. Plaintiff and the other Class members are also entitled to injunctive relief in the form of adequate and sufficient notification of the Data Breach.

COUNT XXIV
Tennessee Social Security Number Protection Act,
Tenn. Code § 47-18-2110
(On Behalf of the Tennessee Class)

302. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

303. Under Tennessee Code § 47-18-2110 any person engaged in any business that has obtained a federal Social Security number "shall make reasonable efforts to protect that social

security number from disclosure to the public." Such persons are prohibited from posting or displaying social security numbers in public, transmitting over the Internet unless secured and encrypted.

304. ComplyRight violated the provisions of § 47-18-2110 in failing to implement and maintain reasonable and adequate security over the Personal Information, which includes social security numbers of Plaintiff and the other Class members.

305. As a result of ComplyRight's unlawful conduct, Plaintiff and the other Class members have suffered and will continue to suffer actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT XXV
Wisconsin Deceptive Trade Practices Act
(On Behalf of the Wisconsin Class)

306. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

307. Section 100.18(1) provides that no person or corporation, with intent to sell, distribute, or increase the consumption of anything offered by it to the public, shall place before the public a statement that contains any assertion or statement of fact that is untrue, deceptive or misleading.

308. ComplyRight misrepresented the quality and extent of its security procedures and its certifications with respect to the handling and maintenance of sensitive information.

309. ComplyRight intended that Plaintiff Newman and the other Class members, as well as others rely on its misrepresentations in deciding to do business with ComplyRight.

310. As a result of ComplyRight's unlawful conduct, Plaintiff and the other Class members have suffered and will continue to suffer actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

COUNT XXVI
Notice of Unauthorized Acquisition of Personal Information,
Wis. Stat. §§ 134.98, *et seq.*
(On Behalf of the Wisconsin Class)

311. Plaintiffs incorporate paragraphs 1–73 as if fully set forth herein.

312. ComplyRight maintains or licenses Personal Information as defined by Wis. Stat. § 134.98(2).

313. Plaintiff Newman's and the Class members' Personal Information includes Personal Information covered under § 134-98(1)(b).

314. ComplyRight violated § 134.98 by failing to notify Plaintiff and the other Class members of the Data Breach in the most expedient time possible and without unreasonable delay. ComplyRight learned of the Data Breach as early as May 22, 2018, but reasonably should have discovered it much earlier. Upon learning of the Data Breach, it failed to disseminate the required notification to Plaintiff and the other Class members until July 13, 2018.

315. Furthermore, the notification was insufficient, misleading, and not compliant with the law. It misrepresented the risks caused by the Data Breach, it had the appearance of a scam, and failed to provide adequate responses to inquiries by concealing the Data Breach from all other media and public forums. To the extent that the Data Breach happened to efile4biz, or other website, ComplyRight failed to accurately and sufficiently identify the relevant data collector.

316. As a result of ComplyRight's unlawful conduct, Plaintiff and the other Class members have suffered and will continue to suffer actual damages, including identity theft, improper disclosure of their Personal Information, lost value of their Personal Information, lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft that resulted and continues to face them.

317. Plaintiff and the other Class members are also entitled to injunctive relief in the form of adequate and sufficient notification of the Data Breach.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all claims so triable.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Classes proposed in this Consolidated Amended Class Action Complaint, respectfully request that the Court enter judgment in their favor and against ComplyRight, as follows:

A. Certifying the Classes as requested herein, designating Plaintiffs as Class Representatives, and appointing Class Counsel as requested in Plaintiffs' motion for class certification;

B. Ordering ComplyRight to pay actual damages to Plaintiffs and the other Class members;

C. Ordering ComplyRight to pay punitive damages, as allowable by law, to Plaintiffs and the other Class members;

D. Ordering ComplyRight to pay Plaintiffs' attorneys' fees, costs, and expenses;

E. Ordering ComplyRight to provide equitable relief, in the form of disgorgement and restitution, and injunctive relief;

F. Ordering ComplyRight to pay both pre- and post-judgment interest on any amounts awarded; and

G. Ordering such other and further relief as may be just and proper.

Dated: September 10, 2018

Respectfully submitted,

/s/ Ben Barnow

Ben Barnow
Erich P. Schork
Jeffrey D. Blake
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Tel: (312) 621-2000
Fax: (312)-641-5504
b.barnow@barnowlaw.com
e.schork@barnowlaw.com
j.blake@barnowlaw.com

Laurence D. King (*pro hac vice* to be sought)
Matthew B. George (*pro hac vice* to be sought)
KAPLAN FOX & KILSHEIMER LLP
350 Sansome Street, Suite 400
San Francisco, CA 94104
Telephone: (415) 772-4700
Facsimile: (415) 772-4707
lking@kaplanfox.com
mgeorge@kaplanfox.com

Aron D. Robinson
LAW OFFICES OF ARON D. ROBINSON
180 W. Washington, Suite 700
Chicago, IL 60602
Tel: (312) 857-9050
Fax: (312) 857-9054
adroblaw@aol.com

Benjamin F. Johns (*pro hac vice* to be sought)
Mark B. DeSanto (*pro hac vice* to be sought)
CHIMICLES & TIKELLIS LLP
One Haverford Centre
361 W. Lancaster Avenue
Haverford, PA 19041
Telephone: 610-642-8500
bfj@chimicles.com
mbd@chimicles.com

Jeremiah Frei-Pearson (*pro hac vice* to be sought)
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
445 Hamilton Avenue, Suite 605
White Plains, New York 10601
Tel: (914) 298-3281
Fax: (914) 824-1561
jfrei-pearson@fbfglaw.com

Matt Harman (*pro hac vice* to be sought)
HARMAN LAW FIRM
3414 Peachtree Road NE Suite 1250
Atlanta, GA 30326
Tel: (404) 554-0777
mharman@harmanlaw.com

David C. O'Mara (*pro hac vice* to be sought)
THE O'MARA LAW FIRM
311 East Liberty Street
Reno, NV 89501
david@omaralaw.net

Shpetim Ademi (*pro hac vice* to be sought)
ADEMI & O'REILLY, LLP
3620 East Layton Avenue
Cudahy, WI 53110
(414) 482-8000
(414) 482-8001 (fax)
sademi@ademilaw.com

Marc A. Wites (*pro hac vice* to be sought)
WITES LAW FIRM
4400 North Federal Highway
Lighthouse Point, FL 33064
Telephone: (954) 933-4400
mwites@witeslaw.com

Attorneys for Plaintiffs

CERTIFICATE OF COMPLIANCE

I hereby certify that on September 10, 2018, the foregoing document was filed with the Court's CM/ECF system, which will provide notice of electronic filing to all counsel of record.

/s/ Ben Barnow